DOCUMENTATION TECHNIQUE

Installation et configuration de CrowdSec

Ayoub MOURKIA

Introduction

CrowdSec est une solution de cybersécurité open source qui analyse les journaux système et applicatifs, détecte des comportements malveillants et applique des décisions de remédiation à l'aide de composants appelés bouncers.

Contrairement à une simple blocklist statique, CrowdSec s'appuie sur des scénarios de détection, des collections de parsers et une API locale (LAPI) pour corréler les événements. Le moteur peut ensuite bannir une adresse IP via un pare-feu, ou protéger une application web à l'aide d'un bouncer WAF adapté.

- Détection comportementale sur les logs.
- Blocage automatique des IP malveillantes.
- Support de nombreux services : SSH, Nginx, Apache, Traefik, etc.
- Gestion locale via cscli et intégration possible avec la console CrowdSec.

Architecture de CrowdSec

- Security Engine : lit les logs, parse les événements et déclenche les scénarios.
- LAPI (Local API) : centralise les décisions et sert d'interface locale aux bouncers.
- Collections : paquets contenant parsers, scénarios et enrichisseurs adaptés à un service.
- Bouncers / Remediation Components : appliquent concrètement les décisions (firewall, Nginx, Traefik, HAProxy...).

Important : Le Security Engine seul détecte mais ne bloque pas. Pour la remédiation, il faut installer un bouncer adapté au service protégé.

Prérequis

- Serveur Linux Debian ou Ubuntu à jour.
- Accès root ou privilèges sudo.
- Connexion Internet pour récupérer les paquets CrowdSec.
- Horloge système synchronisée (NTP recommandé).
- Pare-feu local compatible si utilisation du firewall bouncer : iptables ou nftables.
- Présence de logs exploitables : auth.log, journaux Nginx/Apache, logs applicatifs, etc.

Recommandations avant installation

- Effectuer les mises à jour système avant l'installation.
- Identifier les services à protéger : SSH, Nginx, Apache, reverse proxy, applications métier.
- Vérifier les chemins de logs attendus.
- Prévoir une allowlist pour l'adresse IP d'administration afin d'éviter un bannissement accidentel.

```
sudo apt update && sudo apt full-upgrade -y
sudo reboot
```

Installation du dépôt CrowdSec

La méthode recommandée consiste à ajouter le dépôt officiel CrowdSec puis à installer les paquets depuis ce dépôt.

Méthode rapide

```
curl -s https://install.crowdsec.net | sudo sh
```

Méthode manuelle (Debian / Ubuntu)

```
sudo apt update
sudo apt install -y curl gnupg apt-transport-https
sudo mkdir -p /etc/apt/keyrings
curl -fsSL https://packagecloud.io/crowdsec/crowdsec/gpgkey | gpg --dearmor | sudo tee
/etc/apt/keyrings/crowdsec_crowdsec-archive-keyring.gpg > /dev/null
echo "deb [signed-by=/etc/apt/keyrings/crowdsec_crowdsec-archive-keyring.gpg]
https://packagecloud.io/crowdsec/crowdsec/any any main" | sudo tee
/etc/apt/sources.list.d/crowdsec_crowdsec.list
echo "deb-src [signed-by=/etc/apt/keyrings/crowdsec_crowdsec-archive-keyring.gpg]
https://packagecloud.io/crowdsec/crowdsec/any any main" | sudo tee -a
/etc/apt/sources.list.d/crowdsec_crowdsec.list
sudo apt update
```

Vérification de la version candidate

```
apt list crowdsec
apt-cache policy crowdsec
```

Attention : Sur certaines versions Ubuntu avec ESM/Pro, il peut être nécessaire de définir une priorité APT pour forcer le paquet du dépôt CrowdSec officiel.

```
sudo nano /etc/apt/preferences.d/crowdsec

Package: *
Pin: release o=packagecloud.io/crowdsec/crowdsec,a=any,n=any,c=main
Pin-Priority: 1001

sudo apt update
apt-cache policy crowdsec
```

Installation du moteur CrowdSec

```
sudo apt install crowdsec -y
```

À l'installation, CrowdSec déploie le Security Engine et la LAPI. Un assistant peut détecter automatiquement certains services courants et installer les collections correspondantes.

Vérification du service

```
sudo systemctl status crowdsec
sudo systemctl enable crowdsec
```

- Le service doit apparaître en active (running).
- En cas d'erreur, consulter le journal /var/log/crowdsec.log.

Fichiers et répertoires importants

Chemin	Rôle
/etc/crowdsec/config.yaml	Configuration principale du moteur et de la LAPI
/etc/crowdsec/acquis.yaml	Fichier historique d'acquisition
/etc/crowdsec/acquis.d/*.yaml	Déclarations d'acquisition par service
/etc/crowdsec/bouncers/*.yaml	Configuration des bouncers
/etc/crowdsec/collections/	Collections installées
/var/log/crowdsec.log	Journal du service CrowdSec

Contrôle de santé après installation

Vérifier les acquisitions et les parsers

```
sudo cscli metrics show acquisition parsers
```

Lister les collections, parsers et scénarios

```
sudo cscli collections list
sudo cscli parsers list
sudo cscli scenarios list
```

Si le service attendu n'apparaît pas, il faut installer manuellement la collection correspondante puis vérifier les acquisitions.

Gestion des collections

Les collections regroupent les éléments nécessaires à l'analyse d'un service.

```
sudo cscli collections list
sudo cscli collections install crowdsecurity/linux
sudo cscli collections install crowdsecurity/sshd
sudo cscli collections install crowdsecurity/nginx
sudo systemctl reload crowdsec
```

Conseil : Utiliser uniquement les collections utiles à l'environnement afin de garder une configuration lisible et maîtrisée.

Acquisition des logs

CrowdSec doit savoir quels fichiers de logs lire. Depuis les versions récentes, certains services peuvent être détectés automatiquement, mais il reste indispensable de vérifier les chemins réellement surveillés.

```
sudo cscli metrics show acquisition
```

Ajouter une nouvelle acquisition

```
sudo mkdir -p /etc/crowdsec/acquis.d
sudo nano /etc/crowdsec/acquis.d/nginx.yaml

filenames:
  - /var/log/nginx/access.log
  - /var/log/nginx/error.log
labels:
  type: nginx

sudo crowdsec -t
sudo systemctl restart crowdsec
```

Exemple pour SSH

```
sudo nano /etc/crowdsec/acquis.d/sshd.yaml

filenames:
  - /var/log/auth.log
labels:
  type: syslog

sudo crowdsec -t
sudo systemctl restart crowdsec
```

Installation de la remédiation firewall

Pour protéger des services d'infrastructure comme SSH, SMTP ou une base de données, le firewall bouncer est le composant le plus simple et le plus adapté.

Identifier le backend pare-feu

```
iptables -V
```

Si la sortie contient la mention nf_tables, le système utilise nftables. Sinon, il est généralement en mode iptables classique.

Installation du package

```
# iptables
sudo apt install crowdsec-firewall-bouncer-iptables -y

# nftables
sudo apt install crowdsec-firewall-bouncer-nftables -y
```

Vérification du bouncer

```
sudo systemctl status crowdsec-firewall-bouncer
sudo cscli bouncers list
```

Le bouncer doit apparaître comme valide, avec un dernier pull API récent.

Principe de fonctionnement du firewall bouncer

- Le bouncer interroge la LAPI locale.
- Il récupère les décisions de type ban, captcha ou challenge selon le composant.
- Il alimente des règles de filtrage côté pare-feu.
- Les décisions expirent automatiquement à la fin de leur durée de vie.

Tests de fonctionnement

Test de détection SSH

```
ssh crowdsec-test-NtktlJHV4TfBSK3wvlhiOBnl@<IP_DU_SERVEUR>
sudo cscli alerts list -s crowdsecurity/ssh-generic-test
```

Test de remédiation manuel

Avertissement : Ce test peut bloquer temporairement votre propre accès. Utiliser une IP de test ou régler une durée très courte.

```
curl api.ipify.org
sudo cscli decisions add --ip <VOTRE_IP_PUBLIQUE> --duration 1m --reason "CrowdSec remediation test"
sudo cscli decisions list
```

Après quelques secondes, l'accès au service protégé depuis cette IP doit être bloqué. Une fois la minute écoulée, la décision doit disparaître automatiquement.

Gestion des décisions

```
sudo cscli decisions list
sudo cscli decisions add --ip 203.0.113.10 --duration 4h --reason "Blocage manuel"
sudo cscli decisions delete --ip 203.0.113.10
```

Allowlist / Whitelist

Pour éviter les faux positifs, il est recommandé de déclarer les IP d'administration ou certains réseaux internes dans une allowlist.

```
sudo cscli allowlist create admin_allowlist -d "IP d'administration"
sudo cscli allowlist add admin_allowlist 198.51.100.25
sudo cscli allowlist add admin_allowlist 192.168.1.0/24
sudo cscli allowlist inspect admin_allowlist
sudo systemctl reload crowdsec
```

Exploitation quotidienne

- Consulter les alertes détectées : sudo cscli alerts list
- Consulter les décisions actives : sudo cscli decisions list
- Contrôler les bouncers enregistrés : sudo cscli bouncers list
- Vérifier la connexion à la Central API : sudo cscli capi status
- Contrôler les acquisitions et parsers : sudo cscli metrics show acquisition parsers

Mise à jour

```
sudo apt update
sudo apt upgrade -y
sudo systemctl restart crowdsec
```

Après une mise à jour, vérifier l'état du service, les acquisitions et le bon fonctionnement des bouncers.

Intégration possible avec un serveur web

Pour un serveur web exposé, le firewall bouncer reste utile pour le blocage IP, mais il est préférable d'ajouter un bouncer WAF compatible avec le reverse proxy utilisé.

- Nginx : crowdsec-nginx-bouncer
- OpenResty : crowdsec-openresty-bouncer
- Traefik : traefik-bouncer-plugin
- HAProxy : cs-haproxy-spoa-bouncer

Bonnes pratiques : Sur un service web, il est possible d'utiliser à la fois un firewall bouncer pour la couche réseau et un bouncer WAF pour l'inspection HTTP.

Dépannage

Le service CrowdSec ne démarre pas

```
sudo systemctl status crowdsec
sudo journalctl -u crowdsec -xe
less /var/log/crowdsec.log
```

Aucune ligne lue dans les métriques

- Vérifier les chemins de logs dans /etc/crowdsec/acquis.d/.
- Contrôler les droits de lecture des fichiers.
- Générer de l'activité sur le service puis relancer la vérification.
- Tester la configuration avec sudo crowdsec -t.

Le bouncer n'applique pas les décisions

- Vérifier que le bouncer est listé et valide avec sudo cscli bouncers list.
- Contrôler l'URL LAPI et la clé d'authentification dans le fichier du bouncer.
- S'assurer que le service crowdsec-firewall-bouncer est actif.
- Vérifier que le backend pare-feu installé correspond bien au système.

Faux positifs

- Créer une allowlist pour les IP de confiance.
- Vérifier la pertinence des collections installées.
- Analyser les alertes remontées avant d'ajouter des exclusions larges.

Conclusion

CrowdSec permet de mettre en place une détection moderne et collaborative tout en conservant une logique d'administration simple sur Linux. Une installation propre repose sur quatre points : dépôt officiel, collections adaptées, acquisitions correctement configurées et remédiation testée.

Dans une infrastructure réelle, il est recommandé de commencer par la protection SSH et des services exposés, puis d'étendre progressivement la solution aux reverse proxies, applications web et serveurs mutualisés.

Annexe – Commandes essentielles

```
sudo systemctl status crowdsec
sudo cscli collections list
sudo cscli metrics show acquisition parsers
sudo cscli alerts list
sudo cscli decisions list
sudo cscli bouncers list
sudo cscli capi status
sudo crowdsec -t
```

Annexe – Sources officielles utilisées pour cette procédure

- Documentation CrowdSec – installation Linux
- Documentation CrowdSec – firewall bouncer
- Documentation CrowdSec – health check
- Documentation CrowdSec – acquisition des logs
- Documentation CrowdSec – allowlists / whitelists